

WHAT IS CLAIMED IS:

Sub
a1

5

1. An input device for securing a token from an unauthorized user:
a user interface for accepting entry of a personal identifier from a user;
a processor, communicatively coupled to the user interface;
a token interface, including:

a token interface emitter, for producing a signal having information including the personal identifier, the token interface emitter communicatively coupled to the processor and further communicatively coupled to a token sensor when the token is physically coupled with the token interface; and

10

a shield, substantially opaque to the signal, for substantially confining reception of the signal to the token sensor.

15

2. The input device of claim 1, wherein the token interface emitter is communicatively decoupled from the token sensor when the token is not physically coupled with the token interface.

3. The input device of claim 1, wherein the token interface includes a USB port.

20

4. The input device of claim 1, wherein the shield substantially circumscribes the token interface emitter.

25

5. The input device of claim 1, wherein the token interface further comprises:
a token interface sensor configured to receive the signal produced by a token emitter when the token is physically coupled with the token interface.

30

6. The input device of claim 5, wherein the token emitter emits a second signal including information describing the intensity of the signal.

7. The input device of claim 6, wherein the processor controls the intensity of the first signal according to the information describing intensity of the first signal received from the second signal.

5 8. A method of securing a token having a USB-compliant interface from unauthorized use, comprising the steps of:

accepting the token in an input device having a token interface;
accepting a user-entered personal identifier in the input device; and
transmitting the user-entered personal identifier to the token via a

10 communication path distinct from the USB-compliant interface.

9. The method of claim 8, wherein the step of transmitting the user entered personal identifier to the token via a communication path independent from the USB-compliant interface comprises the steps of:

15 generating a first signal having information including the user-entered personal identifier; and

emitting the generated signal in the token interface for reception by a token sensor.

20 10. The method of claim 9, further comprising the step of receiving the generated first signal in a token sensor.

11. The method of claim 9, wherein the step of accepting the token in a input device having a token interface including a USB compliant port comprises
25 the steps of:

shielding the signal to confine reception of the signal to the sensor.

12. The method of claim 9, wherein:
the method further comprises the step of determining if the token is
accepted in the device; and
the user-entered personal identifier is transmitted to the token via a
5 communication path independent from the USB-compliant interface only if the
token is determined to be accepted by the input device.

13. The method of claim 12, wherein the step of determining if the
token is accepted in the input device comprises the step of sensing a connect
10 signal.

14. The method of claim 12, wherein the step of determining if the
token has been accepted by the input device comprises the step of:
receiving a second signal produced by a token emitter when the token is
15 accepted by the token interface.

15. The method of claim 12, wherein the step of determining if the
token has been accepted by the input device comprises the step of:
receiving a second signal produced by a token emitter after the token
20 sensor receives a third signal in the token interface.

16. The method of claim 9, further comprising the steps of:
receiving a second signal produced by a token emitter, the second signal
including information describing the intensity of the first signal; and
25 controlling the intensity of the first signal according to the information
describing the intensity of the first signal received from the second signal.

17. The method of claim 8, further comprising the steps of:
disabling transmission of the user-entered personal identifier until
30 detection of the acceptance of the token to the USB port.